

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2004年2月12日 (12.02.2004)

PCT

(10) 国際公開番号
WO 2004/013755 A1

- (51) 国際特許分類⁷: G06F 11/00
- (21) 国際出願番号: PCT/JP2003/009894
- (22) 国際出願日: 2003年8月4日 (04.08.2003)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願2002-227888 2002年8月5日 (05.08.2002) JP
- (71) 出願人 (米国を除く全ての指定国について): 財団
法人大阪産業振興機構 (OSAKA INDUSTRIAL PRO-
MOTION ORGANIZATION) [JP/JP]; 〒541-0053 大阪
府 大阪市 中央区本町1-4-5 Osaka (JP).
- (72) 発明者; および
- (75) 発明者/出願人 (米国についてのみ): 斉藤 和典

(SAITO, Kazunori) [JP/JP]; 〒567-0047 大阪府 茨木市
美穂ヶ丘 5番1号 大阪大学内 Osaka (JP).

(74) 代理人: 河野 登夫 (KOHNO, Takao); 〒540-0035 大阪
府 大阪市 中央区 釣鐘町二丁目4番3号 河野特許事
務所 Osaka (JP).

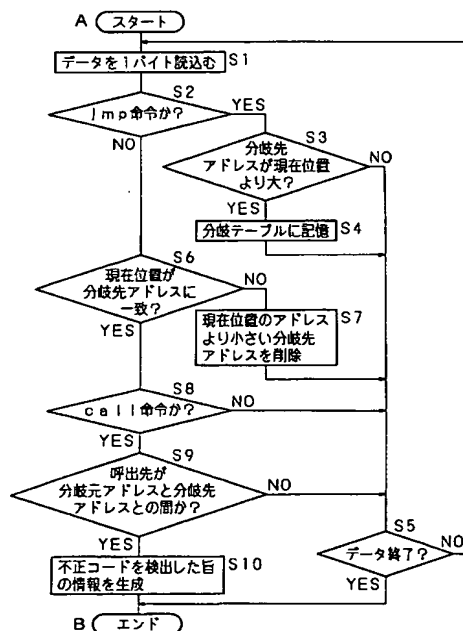
(81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB,
BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK,
DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU,
ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT,
LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO,
NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK,
SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC,
VN, YU, ZA, ZM, ZW.

(84) 指定国 (広域): ARIPO 特許 (GH, GM, KE, LS, MW, MZ,
SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア特許 (AM,
AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許

[続葉有]

(54) Title: DATA PROCESSING METHOD, DATA PROCESSING DEVICE, COMPUTER PROGRAM, AND RECORDING MEDIUM

(54) 発明の名称: データ処理方法、データ処理装置、コンピュータプログラム、及び記録媒体



A...START
S1...READ IN 1 BYTE OF DATA
S2...JUMP INSTRUCTION?
S3...JUMP DESTINATION ADDRESS IS GREATER THAN
THE CURRENT POSITION?
S4...STORE IN THE JUMP TABLE
S6...CURRENT POSITION COINCIDES WITH THE JUMP
DESTINATION ADDRESS?
S7...DELETE JUMP DESTINATION ADDRESS SMALLER
THAN THE CURRENT POSITION ADDRESS
S8...CALL INSTRUCTION?
S9...CALL DESTINATION BETWEEN JUMP ORIGIN
ADDRESS AND JUMP DESTINATION ADDRESS?
S10...GENERATE INFORMATION THAT UNAUTHORIZED
CODE HAS BEEN DETECTED
S5...DATA END?
B...END

(57) Abstract: A jump origin address and a jump destination address of a jump instruction (jmp instruction) are stored. It is judged whether a call instruction for calling an instruction code group for executing an external command is related to the jump destination address. When a call instruction is related to the jump destination address, it is judged whether the call destination is located between the jump origin address and the jump destination address. When the call destination by the call instruction is located between the jump origin address and the jump destination address, information that an unauthorized code has been detected is generated.

[続葉有]



(AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

添付公開書類:

— 国際調査報告書

(57) 要約: 分岐命令 (j m p 命令) の分岐元アドレスと分岐先アドレスとを記憶し、分岐先アドレスに外部コマンドを実行させるための命令コード群を呼出するための呼出命令 (c a l l 命令) が対応付けられているか否かを判断し、呼出命令が分岐先アドレスに対応付けられている場合、その呼出先が分岐元アドレスと分岐先アドレスとの間にあるか否かを判断し、呼出命令による呼出先が分岐元アドレスと分岐先アドレスとの間にある場合、不正コードを検出した旨の情報を生成する。

明 細 書

データ処理方法、データ処理装置、コンピュータプログラム、
及び記録媒体

技術分野

本発明は、不正な処理を実行するデータを検出するデータ処理方法、データ処理装置、該データ処理装置を実現するためのコンピュータプログラム、及び該コンピュータプログラムが記録されているコンピュータでの読取りが可能な記録媒体に関する。

背景技術

インターネット網の普及に伴い、各種の情報処理装置がコンピュータウィルス、クラッキング等の攻撃の対象となり、それらの脅威に晒される可能性が高くなってきている。

例えば、近年、「ニムダ」、「コードレッド」等のコンピュータウィルスに代表されるように、システムプログラム又はウェブブラウザのようなアプリケーションプログラムの脆弱性（セキュリティホール）を利用して自己増殖させ、甚大な被害を与えたケースが存在する。

前述のようなコンピュータウィルス、クラッキング等による攻撃では、不正な処理を行う命令コード（以下、不正コードという）を含む攻撃データを攻撃対象であるサーバ装置、パーソナルコンピュータ等の情報処理装置に対して送信し、その情報処理装置にて前記命令コードが実行されるようにしている。このような攻撃手法は様々なものが存在し、その１つとしてバッファオーバーフローによる攻撃手法が知られている。バッファオーバーフローでは、スタック内に確保されたバッファにおいて、確保されたバッファ以上のスタッ

クエリアに書込みが行われている状態であり、バッファオーバーフローの状態に陥った場合、予期せぬ変数破壊を招き、プログラムの誤動作の原因となり得る。バッファオーバーフローによる攻撃では、プログラムの誤動作を意図的に引き起し、例えばシステムの管理者権限を取得することが行われる。

これらのコンピュータウイルス、クラッキング等の攻撃に対処するため、従来では、受信したデータに対して不正コードにみられる特定のビットパターンの有無を検出する。そして、そのようなビットパターンが受信したデータに含まれている場合には、不正コードを含んだ攻撃データであると判定し、データの受信拒否、ユーザへの報知等の処理を行うようにしている。

そのため、従来の手法により様々なコンピュータウイルス、クラッキング等の攻撃に対処するためには、各コンピュータウイルス、クラッキングに対応した特定のビットパターンをデータベースに記憶させて予め用意しておく必要があり、新種のコンピュータウイルス、クラッキング手法が発見された場合には、前記データベースを更新して対処しなければならない。

ところで、攻撃データに対する従来の検出方法では、前述のように既知のビットパターンを検出するか、又はNOP命令（NOP：non-operation）の単純な繰り返しといった攻撃処理にとって、本質的とはいえない部分の構造を検出するようにしてきた。そのため、攻撃データのバリエーションに弱く、未知の攻撃データが現れる毎に、検出に用いるビットパターンのデータベースを更新する必要があり、データベースが更新されるまでのタイムラグが問題になっていた。

発明の開示

本発明は斯かる事情に鑑みてなされたものであり、分岐命令に係

る命令コードを入力されたデータから検索し、分岐先アドレスに、所定の処理を実行する命令コード群を呼出するための命令コードが対応付けられているか否かを判断し、分岐先アドレスに前記命令コードが対応付けられていると判断した場合、前記命令コードの呼出先アドレスが前記分岐元アドレス及び分岐先アドレスの間にあるか否かを判断する構成とすることにより、不正な処理を行う命令コード群を検出するためのビットパターンを予め用意する必要がなく、不正な処理を行う未知の命令コード群に対しても検出可能なデータ処理方法、データ処理装置、該データ処理装置を実現するためのコンピュータプログラム、及び該コンピュータプログラムが記録されているコンピュータでの読取りが可能な記録媒体を提供することを目的とする。

第1発明に係るデータ処理方法は、複数の命令コードを含むデータの入力を受付け、受付けたデータに含まれる命令コードに基づいて実行される処理が不正処理であるか否かを判断するデータ処理方法において、分岐命令に係る命令コードを前記データから検索し、検索された命令コードに対応付けられている分岐元アドレス、及び前記命令コードの分岐先に対応付けられている分岐先アドレスを記憶し、前記分岐先アドレスに、所定の処理を実行する命令コード群を呼出するための命令コードが対応付けられているか否かを判断し、前記分岐先アドレスに前記命令コードが対応付けられていると判断した場合、前記命令コードの呼出先アドレスを記憶し、記憶した呼出先アドレスが前記分岐元アドレス及び分岐先アドレスの間にあるか否かを判断することを特徴とする。

第2発明に係るデータ処理装置は、複数の命令コードを含むデータの入力を受付ける手段を備え、該手段にて受付けたデータに含まれる命令コードに基づいて実行される処理が不正処理であるか否か

を判断するデータ処理装置において、分岐命令に係る命令コードを前記データから検索する手段と、検索された命令コードに対応付けられている分岐元アドレス、及び前記命令コードの分岐先に対応付けられている分岐先アドレスを記憶する手段と、前記分岐先アドレスに、所定の処理を実行する命令コード群を呼出するための命令コードが対応付けられているか否かを判断する手段と、前記分岐先アドレスに前記命令コードが対応付けられていると判断した場合、前記命令コードの呼出先アドレスを記憶する手段と、記憶した呼出先アドレスが前記分岐元アドレス及び分岐先アドレスの間にあるか否かを判断する手段と、前記呼出先アドレスが前記分岐元アドレス及び分岐先アドレスの間にある場合、前記データが不正処理を実行するデータである旨の情報を出力する手段とを備えることを特徴とする。

第3発明に係るデータ処理装置は、第2発明に係るデータ処理装置において、前記命令コード群の復帰先アドレスに所定の文字列が対応付けられているか否かの判断をする手段を更に備え、前記文字列が前記復帰先アドレスに対応付けられている場合、前記データが不正処理を実行するデータである旨の情報を出力すべくしてあることを特徴とする。

第4発明に係るデータ処理装置は、複数の命令コードを含むデータの入力を受付ける手段を備え、該手段にて受付けたデータに含まれる命令コードに基づいて実行される処理が不正処理であるか否かを判断するデータ処理装置において、所定の処理を実行する命令コード群を呼出するための命令コードを前記データから検索する手段と、前記命令コード群の復帰先アドレスに所定の文字列が対応付けられているか否かを判断する手段と、前記文字列が前記復帰先アドレスに対応付けられている場合、前記データが不正処理を実行するデータである旨の情報を出力する手段とを備えることを特徴とする。

第5発明に係るデータ処理装置は、複数の命令コードを含むデータの入力を受付ける手段を備え、該手段にて受付けたデータに含まれる命令コードに基づいて実行される処理が不正処理であるか否かを判断するデータ処理装置において、所定の処理を実行する命令コード群を呼出するための命令コードを前記データから検索する手段と、前記命令コードが検索された場合、前記命令コード群の復帰先アドレスを取得するための命令コードが前記命令コード群に含まれるか否かを判断する手段と、前記命令コードが前記命令コード群に含まれる場合、前記データが不正処理を実行するデータである旨の情報を出力する手段とを備えることを特徴とする。

第6発明に係るコンピュータプログラムは、コンピュータに、入力された複数の命令コードを含むデータに基づいて実行される処理が不正処理であるか否かを判断させるステップを有するコンピュータプログラムにおいて、コンピュータに、分岐命令に係る命令コードを前記データから検索させるステップと、コンピュータに、検索された命令コードに対応付けられている分岐元アドレス、及び前記命令コードの分岐先に対応付けられている分岐先アドレスを記憶させるステップと、コンピュータに、前記分岐先アドレスに、所定の処理を実行する命令コード群を呼出するための命令コードが対応付けられているか否かを判断させるステップと、コンピュータに、前記分岐先アドレスに前記命令コードが対応付けられていると判断した場合、前記命令コードの呼出先アドレスを記憶させるステップと、コンピュータに、記憶させた呼出先アドレスが前記分岐元アドレス及び分岐先アドレスの間にあるか否かを判断させるステップとを有することを特徴とする。

第7発明に係るコンピュータでの読取りが可能な記録媒体は、コンピュータに、入力された複数の命令コードを含むデータに基づい

て実行される処理が不正処理であるか否かを判断させるステップを有するコンピュータプログラムが記録されているコンピュータでの読取りが可能な記録媒体において、コンピュータに、分岐命令に係る命令コードを前記データから検索させるステップと、コンピュータに、検索された命令コードに対応付けられている分岐元アドレス、及び前記命令コードの分岐先に対応付けられている分岐先アドレスを記憶させるステップと、コンピュータに、前記分岐先アドレスに、所定の処理を実行する命令コード群を呼出するための命令コードが対応付けられているか否かを判断させるステップと、コンピュータに、前記分岐先アドレスに前記命令コードが対応付けられていると判断した場合、前記命令コードの呼出先アドレスを記憶させるステップと、コンピュータに、記憶させた呼出先アドレスが前記分岐元アドレス及び分岐先アドレスの間にあるか否かを判断させるステップと有するコンピュータプログラムが記録されていることを特徴とする。

第1発明、第2発明、第6発明、及び第7発明にあっては、分岐命令に係る命令コードを入力されたデータから検索し、検索された命令コードの分岐元アドレス及び分岐先アドレスを記憶し、分岐先アドレスに、所定の処理を実行する命令コード群を呼出するための命令コードが対応付けられているか否かを判断し、分岐先アドレスに前記命令コードが対応付けられていると判断した場合、命令コードの呼出先アドレスを記憶し、記憶した呼出先アドレスが分岐元アドレス及び分岐先アドレスの間にあるか否かを判断するようにしている。したがって、通常のデータ（実行コード）には見られない普遍的な構造に着目しているため、不正コードを変形させた場合であっても検出できる可能性が高く、未知の攻撃データが現れたときでも、不正コードの本質的処理が変わらない限り、不正コードを見抜くことができる。また、命令コードを逐次的に読込むことによって、不

正コードであるか否かの判定が可能であるため処理速度が速く、例えば通信により受信したデータに対してリアルタイムに判定することができる。

第3発明にあっては、命令コード群の復帰先アドレスに所定の文字列が対応付けられているか否かの判断をする手段を更に備えているため、不正コードの検出精度が向上する。

第4発明にあっては、所定の処理を実行する命令コード群を呼出するための命令コードを入力されたデータから検索し、命令コード群の復帰先アドレスに所定の文字列が対応付けられているか否かを判断するため、不正コードであるか否かの判定が簡単であり、しかも精度良く判定することができる。

第5発明にあっては、所定の処理を実行する命令コード群を呼出するための命令コードを入力されたデータから検索し、前記命令コードが検索された場合、命令コード群に復帰先アドレスを取得するための命令コードが含まれるか否かを判断するため、不正コードであるか否かの判定が簡単であり、しかも精度良く判定することができる。

図面の簡単な説明

第1図は本発明のデータ処理装置を利用した侵入検出システムを説明する模式的構成図、第2図は不正コードの特徴的構造を説明する概念図、第3図は不正コードの特徴的構造を説明する概念図、第4図は本実施の形態に係る侵入検出システムの処理手順を説明するフローチャート、第5図は侵入検出の際に利用される分岐テーブルの一例を示す概念図、第6図は偽装された不正コードの特徴的構造を説明する概念図、第7図は偽装された不正コードの特徴的構造を説明する概念図、第8図は本実施の形態に係る侵入検出システムの

処理手順を説明するフローチャート、第 9 図は本実施の形態に係る侵入検知システムの構成を説明する模式図である。

発明を実施するための最良の形態

以下、本発明をその実施の形態を示す図面に基づいて具体的に説明する。

実施の形態 1.

第 1 図は本発明のデータ処理装置を利用した侵入検出システムを説明する模式的構成図である。図中 10 は本発明のデータ処理装置を具体化した中継装置であり、例えば、ルータ、スイッチ、ブロードバンドルータ等のデータ通信を中継する装置である。中継装置 10 は、CPU 11、メモリ 12、及び通信インターフェース（以下、通信 IF という）13、14 を備えており、通信 IF 13 に接続された情報処理装置 20 とインターネット網のようなデータ通信網 N を介して通信 IF 14 に接続された他の情報処理装置 30 と間で、各種データの送受信を中継する。情報処理装置 20、30 は、例えば、パーソナルコンピュータ、サーバ装置、携帯電話機、PDA（Personal Digital Assistant）等のデータ通信を行うことができる装置である。

情報処理装置 30 から送信されたデータを中継装置 10 が受信した際、中継装置 10 は受信したデータが不正な処理を実行する命令コード（以下、不正コードという）を含んだデータであるか否かを判断し、不正コードを含んでいる場合には、通信の遮断、警報の出力等の処理を行う。

中継装置 10 のメモリ 12 は、ルーティングテーブル 12a、フィルタリングテーブル 12b、及び分岐テーブル 12c を備えている。

ルーティングテーブル 12 a には通信の経路制御情報が記憶されており、該経路制御情報によって、情報処理装置 20 から送信されるデータの伝送経路が決定される。フィルタリングテーブル 12 b には受信を拒否すべき通信相手の識別情報（例えば、IP アドレス又はポート番号等）が記憶されており、前記識別情報に該当する情報処理装置からのデータを受信した場合、そのデータを情報処理装置 20 へ送信しないようにしている。

また、メモリ 12 には本発明のコンピュータプログラムが予め記憶されており、CPU 11 が当該コンピュータプログラムを実行することによって、中継装置 10 は、不正コードを検出する侵入検出システムとして動作する。分岐テーブル 12 c には、前記コンピュータプログラムが起動中に取得した特定の命令コードに係るメモリアドレス（以下、単にアドレスという）が記憶され、不正コードを含んだデータであるか否かを判断する際に利用される。

中継装置 10 の CPU 11 は、これらのテーブルに対して適宜書込み処理、又は読込み処理を行い、通信制御を行うようにしている。

以下、発明者らの知見に基づいて見出された不正コードの特徴的構造について説明する。発明者らは不正コードの普遍的な特徴として、分岐命令（以下、j m p 命令という）により指定された分岐先に呼出命令（以下、c a l l 命令という）が設定されていること、そしてその呼出先が j m p 命令と c a l l 命令との間にあることを見出している。そして、c a l l 命令によって、スタックへ格納されたアドレス、すなわち c a l l 命令の次のアドレスを呼出し先の命令コード群にて取得して、取得したアドレスを用いて起動したいコマンドを実行させるようにしている。

第 2 図及び第 3 図は、不正コードの特徴的構造を説明する概念図である。前述したように、処理を分岐させるための j m p 命令の分

岐先に対応させて `call` 命令を設定している。すなわち、`jmp` 命令の分岐先アドレス (`A10`) に `call` 命令に対応させている。

そして、`call` 命令の呼出し先に、外部コマンドを呼び出すための命令コード群 (`A2`～`A6`) を対応付け、その `call` 命令による呼出し先が、分岐元アドレス (`A1`) と分岐先アドレス (`A10`) との間にくるように設定している。この命令コード群において、`call` 命令によってスタックへ格納されたアドレス、すなわち `call` 命令の次のアドレス (`A11`) を `pop` 命令によって取得し、取得したアドレスを利用して、外部コマンドを実行させるようにしている。

したがって、不正コードの作成者が意図した任意の外部コマンドを `call` 命令の次のアドレスに対応させることによって、これらの命令コードが実行されるときに、前記外部コマンドが呼出されて実行される構成となっている。

なお、前記命令コード群と `call` 命令との間 (`A7`～`A9`) にはダミーの初期データ及び作業領域を設けても良いことは勿論である。

前述した不正コードは、第3図に模式的に示した如く、(1) `jmp` 命令の分岐先に `call` 命令が存在すること、(2) `call` 命令の呼出し先が `call` 命令と `jmp` 命令との間に存在することを特徴としている。

中継装置 10 では、このような特徴的構造を持つ不正コードを通信 IF 14 にて受信したデータから検出し、警報を出力するか又は通信の遮断を行うようにしている。

以下、前述した特徴的構造をもつ不正コードの検出手順について説明する。第4図は本実施の形態に係る侵入検出システムの処理手順を説明するフローチャートであり、第5図は侵入検出の際に利用

される分岐テーブル 12 c の一例を示す概念図である。まず、中継装置 10 の CPU 11 は通信 IF 14 にて受信したデータを 1 バイト読み込む（ステップ S 1）。そして、CPU 11 は、読み込んだデータが jmp 命令か否かを判断する（ステップ S 2）。読み込んだデータが jmp 命令である場合（S 2 : YES）、CPU 11 は、その jmp 命令で指定される分岐先のアドレスが、現在位置のアドレスよりも大きいか否かを判断する（ステップ S 3）。

分岐先のアドレスが現在位置のアドレスよりも大きいと判断した場合（S 3 : YES）、現在位置のアドレス（分岐元アドレス）と分岐先のアドレス（分岐先アドレス）とを対応付けて分岐テーブル 12 c に記憶させる（ステップ S 4）。第 2 図に示した如きデータの例では、アドレス A 1 のデータを読み込んだ場合、そのデータは jmp 命令であり、当該 jmp 命令で指定される分岐先のアドレス（A 1 0）がアドレス A 1 よりも大きいため、分岐元アドレスとして A 1、分岐先アドレスとして A 1 0 が分岐テーブル 12 c に記憶される（第 5 図参照）。

ステップ S 3 にて、分岐先アドレスが現在位置のアドレスよりも小さいと判断した場合（S 3 : NO）、又はステップ S 4 にて、分岐テーブル 12 c に分岐元アドレスと分岐先アドレスとを記憶させた場合、CPU 11 は、読み込むべきデータが終了したか否かを判断し（ステップ S 5）、読み込むべきデータが未だ残っていると判断した場合（S 5 : NO）、処理をステップ S 1 へ戻し、読み込むべきデータが終了したと判断した場合（S 5 : YES）、本ルーチンを終了する。

ステップ S 2 において、読み込んだデータ jmp 命令でないと判断した場合（S 2 : NO）、CPU 11 は、現在位置のアドレスが分岐テーブル 12 c に記憶された分岐先アドレスに一致するか否かを

判断する（ステップ S 6）。現在位置のアドレスが分岐先のアドレスに一致しない場合（S 6 : NO）、現在位置のアドレスより小さい分岐先アドレスを分岐テーブル 1 2 c から削除する（ステップ S 7）。そして、ステップ S 5 の処理を行い、再度ステップ S 1 へ処理を戻すか、又は本ルーチンの処理を終了するか否かの判断をする。

現在位置のアドレスが分岐テーブル 1 2 c に記憶された分岐先アドレスに一致すると判断した場合（S 6 : YES）、CPU 1 1 は、現在位置のアドレスに対応付けられた命令コードが call 命令であるか否かを判断する（ステップ S 8）。現在位置のアドレスに対応付けられた命令コードが call 命令であると判断した場合（S 8 : YES）、CPU 1 1 は、分岐テーブル 1 2 c を参照することによって、前記 call 命令による呼出先が分岐元アドレスと分岐先アドレスとの間にあるか否かを判断する（ステップ S 9）。

ステップ S 8 にて、call 命令でないと判断した場合（S 8 : NO）、又はステップ S 9 にて、呼出先が分岐元アドレスと分岐先アドレスとの間にないと判断した場合（S 9 : NO）、処理をステップ S 5 へ移行させる。

call 命令による呼出先が分岐テーブル 1 2 c に記憶された分岐元アドレスと分岐先アドレスとの間にあると判断した場合（S 9 : YES）、CPU 1 1 は、不正コードを検出した旨の情報を生成する（ステップ S 1 0）。

前述の不正コードを検出した旨の情報は、中継装置 1 0 に液晶ディスプレイ等の表示部を設けて表示させるようにしてもよく、また、ブザー、LED ランプ等の警報部を設けて報知するようにしてもよい。更に、前記情報を情報処理装置 2 0 へ送信し、情報処理装置 2 0 が備える表示部（不図示）にて表示させるようにしてもよい。更に、前記不正コードを検出した旨の情報が生成されたことを受けて

通信を遮断するようにしてもよい。

なお、前述したように `call` 命令によりスタックへ格納されるアドレスには、実行させたい外部コマンドの文字列が存在するため、`call` 命令の次のアドレスにアスキー文字列（コマンド名）が存在するか否かを傍証として利用することにより、不正コードの検出精度を向上させることができる。

また、`call` 命令の次のアドレスにアスキー文字列が存在するか否かについての判断を単独で行うことによっても、不正コードの有無を検出できることが発明者らの検討により知られている。

このように、本実施の形態では、データを逐次的に読んで処理することにより、不正コードが含まれているか否かについて判断できるため、不正コードの有無を検出するアルゴリズムが簡単であり、しかも高速処理が可能である。

実施の形態 2.

前述の不正コードでは、`call` 命令の次のアドレスに実行させたい外部コマンドを置くこと特徴としており、実施の形態 1 では、そのような外部コマンドを呼出すための特殊な構造を見出すことによって、不正コードを検出していた。しかしながら、実行させたい外部コマンドは必ずしも `call` 命令の次に置く必要はなく、不正コードの作者によって予め定められたアドレス分だけ位置をずらして置くことも可能である。このような不正コードをここでは偽装された不正コードと呼び、以下、この偽装された不正コードの特徴的構造、及び検出手順について説明する。なお、中継装置 10 の構成、及び情報処理装置 20, 30 との接続構成は実施の形態 1 と同様であるため説明を省略する。

第 6 図及び第 7 図は偽装された不正コードの特徴的構造を説明する概念図である。偽装された不正コードでも、`call` 命令によっ

て呼出された命令コード群において、起動したい外部コマンドに対応付けられているアドレスを取得するようにしていることは前述と同様であるが、c a l l 命令と外部コマンドとの間に固定長を有するダミーの命令コードを置いて偽装していることが実施の形態 1 で説明した不正コードと異なる。

すなわち、第 6 図に示した構造を有する偽装された不正コードでは、c a l l 命令によりスタックへ格納されたアドレス (A 2) を、A 1 6 ~ A 2 0 に規定された命令コード群にて取得し、そのアドレス A 2 から 5 つ目のアドレス (A 7) に対応付けられている外部コマンドを起動させるようにするのである。

このような偽装された不正コードは、実施の形態 1 で説明した処理によっては検出不可能であるが、第 7 図に模式的に示した如く、
(1) c a l l 命令によって命令コード群を呼出し、(2) その命令コード群において、c a l l 命令によってスタックへ格納したアドレスを p o p 命令により取得するという特徴的構造を依然として有していることが分かる。したがって、c a l l 命令によって呼出された命令コード群において、p u s h 命令が先行しない p o p 命令を検索することによって、偽装された不正コードを検出することが可能となる。

以下、偽装された不正コードの検出手順について説明する。

第 8 図は本実施の形態に係る侵入検出システムの処理手順を説明するフローチャートである。まず、中継装置 1 0 の C P U 1 1 は、受信したデータから c a l l 命令を検索する (ステップ S 2 1)。そして、検索の結果、c a l l 命令があるか否かを判断し (ステップ S 2 2)、c a l l 命令がある場合 (S 2 2 : Y E S)、C P U 1 1 は、検索された c a l l 命令のアドレスをメモリ 1 2 に記憶させる (ステップ S 2 3)。受信したデータに c a l l 命令がない場

合（S 2 2 : N O）、本侵入検出システムによる処理を終了する。

検索された c a l l 命令のアドレスを記憶させた後、その c a l l 命令により指定される呼出先アドレスへ移動させ（ステップ S 2 4）、データを 1 バイト読み込む（ステップ S 2 5）。

次いで、C P U 1 1 は、読み込んだデータがスタックへアドレスを格納するための p u s h 命令か否かを判断する（ステップ S 2 6）。p u s h 命令であると判断した場合（S 2 6 : Y E S）、現在アドレスを記憶して（ステップ S 2 7）、処理をステップ S 2 5 へ戻す。

読み込んだデータが p u s h 命令でないと判断した場合（S 2 6 : N O）、p o p 命令であるか否かを判断する（ステップ S 2 8）。p o p 命令でないと判断した場合（S 2 8 : N O）、呼出先のルーチンが終了したか否かを判断する（ステップ S 3 1）。

呼出先のルーチンが終了していないと判断した場合（S 3 1 : N O）、処理をステップ S 2 5 へ戻し、呼出先のルーチンが終了したと判断した場合（S 3 1 : Y E S）、ステップ S 2 3 にて記憶させたアドレスを参照し、呼出元の次のアドレスへ移動させ（ステップ S 3 2）、c a l l 命令を再度検索し直す。

ステップ S 2 5 で読み込んだデータが p o p 命令であると判断した場合（S 2 8 : Y E S）、C P U 1 1 は、ステップ S 2 7 にて記憶させたアドレスを参照することによって、p u s h 命令が先行しない p o p 命令であるか否かを判断する（ステップ S 2 9）。p u s h 命令が先行しない p o p 命令でないと判断した場合（S 2 9 : N O）、処理をステップ S 3 1 へ移行する。

ステップ S 2 5 で読み込んだデータが、p u s h 命令が先行しない p o p 命令であると判断した場合（S 2 9 : Y E S）、C P U 1 1 は、不正コードを検出した旨の情報を生成する（ステップ S 3 0）。

前述の不正コードを検出した旨の情報は、実施の形態 1 と同様に、

中継装置 10 に液晶ディスプレイ等の表示部を設けて表示させるようにしてもよく、また、ブザー、LED ランプ等の警報部を設けて報知するようにしてもよい。更に、前記情報を情報処理装置 20 へ送信し、情報処理装置 20 が備える表示部（不図示）にて表示させるようにしてもよい。更に、前記不正コードを検出した旨の情報が生成されたことを受けて通信を遮断するようにしてもよい。

実施の形態 3.

前述の実施の形態では、ルータ、スイッチ、ブロードバンドルータ等のデータ通信で利用される中継装置に本発明を適用した形態について説明したが、パーソナルコンピュータ、サーバ装置、携帯電話機、PDA等の通信機能を有した情報処理装置に適用することも可能である。

第 9 図は本実施の形態に係る侵入検知システムの構成を説明する模式図である。図中 50 は、パーソナルコンピュータのような情報処理装置であり、該情報処理装置 50 にはルータのような中継装置 40 を介してデータ通信網 N へ接続されている。情報処理装置 50 は、データ通信網 N 及び中継装置 40 を通じて各種の通信機器、及び他の情報処理装置からデータを受信するとともに、それらの通信機器、情報処理装置へデータを送信するようにしている。

中継装置 40 には、CPU 41、メモリ 42、及び通信 IF 43、44 を備えており、メモリ 42 には、通信の経路制御情報が記憶されたルーティングテーブル 42a と、受信を拒否すべき通信相手の識別情報（例えば、IP アドレス又はポート番号等）が記憶されたフィルタリングテーブル 42b とを有している。情報処理装置 50 から外部へデータを送信する際にルーティングテーブル 42a により伝送経路が設定され、外部からデータを受信する際、フィルタリングテーブル 42b を参照することにより受信を拒否すべき通信相

手であるか否かが判定される。

情報処理装置 50 は、CPU 51 を備えており、バス 52 を介して、ROM 53、RAM 54、表示部 55、入力部 56、通信部 57、補助記憶装置 58、及び内部記憶装置 59 等の各種ハードウェアに接続されている。CPU 51 は、ROM 53 に格納された制御プログラムに従って、それらのハードウェアを制御する。RAM 54 は、SRAM 又はフラッシュメモリ等で構成され、ROM 53 に格納された制御プログラムの実行時に発生するデータを記憶する。

表示部 55 は、CRT、液晶ディスプレイ等の表示装置であり、入力部 56 は、キーボード、マウス等の入力装置である。表示部 55 及び入力部 56 は、例えば、送信すべきデータの入力及び表示をする際に利用される。通信部 57 は、モデム等の回線終端装置を備えており、中継装置 40 を介した各種データの送受信を制御する。

補助記憶装置 58 は、本発明のコンピュータプログラム及びデータを記録したFD、CD-ROM等の記録媒体 60 からコンピュータプログラム及びデータを読取るFDドライブ、CD-ROMドライブ等からなり、読取られたコンピュータプログラム及びデータは、内部記憶装置 59 に記憶される。内部記憶装置 59 に記憶されているコンピュータプログラム及びデータは、RAM 54 に読込まれ、CPU 51 が実行することで本実施の形態に係る情報処理装置 50 として動作する。

なお、本発明のコンピュータプログラムは、記録媒体 60 により提供されるだけでなく、データ通信網 N を通じて提供される形態であってもよいことは勿論である。

前述のコンピュータプログラムは、情報処理装置 50 の起動時に自動的に RAM 54 に読込まれる常駐型のプログラムであることが望ましく、通信部 57 にて外部からデータを受信した際に、自動的

に不正コードを検出するようにしておくといよい。なお、不正コードの検出手順については、実施の形態 1 及び実施の形態 2 で説明した通りであるので説明を省略する。

本実施の形態では、パーソナルコンピュータのような情報処理装置 50 を利用して不正コードを含んだデータを検出する構成としたが、パーソナルコンピュータの他、携帯電話機、PDA、コンピュータゲーム機、車載通信装置、各種の情報家電に適用できることは勿論である。

また、本発明のコンピュータプログラムをFD、CD-ROM等の記録媒体に記録させて提供することにより、コンピュータウィルスを検出するアプリケーションソフトウェアのパッケージとして提供することも可能である。

産業上の利用可能性

以上、詳述したように、分岐命令に係る命令コードを入力されたデータから検索し、検索された命令コードの分岐元アドレス及び分岐先アドレスを記憶し、分岐先アドレスに、所定の処理を実行する命令コード群を呼出すための命令コードが対応付けられているか否かを判断し、分岐先アドレスに前記命令コードが対応付けられていると判断した場合、命令コードの呼出先アドレスを記憶し、記憶した呼出先アドレスが分岐元アドレス及び分岐先アドレスの間にあるか否かを判断するようにしている。したがって、通常の実行コードでは見られない普遍的な構造に着目しているため、不正コードを変形させた場合であっても検出できる可能性が高く、未知の攻撃データが現れたときでも、不正コードの本質的処理が変わらない限り、不正コードを見抜くことができる。また、命令コードを逐次的に読込むことによって、不正コードであるか否かの判定が可能であるた

め処理速度が速く、例えば通信により受信したデータに対してリアルタイムに判定することができる。

また、命令コード群の復帰先アドレスに所定の文字列が対応付けられているか否かの判断をする手段を更に備えているため、不正コードの検出精度が向上する。

また、所定の処理を実行する命令コード群を呼出するための命令コードを入力されたデータから検索し、命令コード群の復帰先アドレスに所定の文字列が対応付けられているか否かを判断するため、不正コードであるか否かの判定が簡単であり、しかも精度良く判定することができる。

更に、所定の処理を実行する命令コード群を呼出するための命令コードを入力されたデータから検索し、前記命令コードが検索された場合、命令コード群に復帰先アドレスを取得するための命令コードが含まれるか否かを判断するため、不正コードであるか否かの判定が簡単であり、しかも精度良く判定することができる等、本発明は優れた効果を奏する。

請 求 の 範 囲

1. 複数の命令コードを含むデータの入力を受付け、受付けたデータに含まれる命令コードに基づいて実行される処理が不正処理であるか否かを判断するデータ処理方法において、

分岐命令に係る命令コードを前記データから検索し、検索された命令コードに対応付けられている分岐元アドレス、及び前記命令コードの分岐先に対応付けられている分岐先アドレスを記憶し、前記分岐先アドレスに、所定の処理を実行する命令コード群を呼出するための命令コードが対応付けられているか否かを判断し、前記分岐先アドレスに前記命令コードが対応付けられていると判断した場合、前記命令コードの呼出先アドレスを記憶し、記憶した呼出先アドレスが前記分岐元アドレス及び分岐先アドレスの間にあるか否かを判断することを特徴とするデータ処理方法。

2. 複数の命令コードを含むデータの入力を受付ける手段を備え、該手段にて受付けたデータに含まれる命令コードに基づいて実行される処理が不正処理であるか否かを判断するデータ処理装置において、

分岐命令に係る命令コードを前記データから検索する手段と、検索された命令コードに対応付けられている分岐元アドレス、及び前記命令コードの分岐先に対応付けられている分岐先アドレスを記憶する手段と、前記分岐先アドレスに、所定の処理を実行する命令コード群を呼出するための命令コードが対応付けられているか否かを判断する手段と、前記分岐先アドレスに前記命令コードが対応付けられていると判断した場合、前記命令コードの呼出先アドレスを記憶する手段と、記憶した呼出先アドレスが前記分岐元アドレス及び分岐先アドレスの間にあるか否かを判断する手段と、前記呼出先アドレスが前記分岐元アドレス及び分岐先アドレスの間にある場合、前

記データが不正処理を実行するデータである旨の情報を出力する手段とを備えることを特徴とするデータ処理装置。

3. 前記命令コード群の復帰先アドレスに所定の文字列が対応付けられているか否かの判断をする手段を更に備え、前記文字列が前記復帰先アドレスに対応付けられている場合、前記データが不正処理を実行するデータである旨の情報を出力すべくなしてあることを特徴とする請求項2に記載のデータ処理装置。

4. 複数の命令コードを含むデータの入力を受付ける手段を備え、該手段にて受付けたデータに含まれる命令コードに基づいて実行される処理が不正処理であるか否かを判断するデータ処理装置において、

所定の処理を実行する命令コード群を呼出するための命令コードを前記データから検索する手段と、前記命令コード群の復帰先アドレスに所定の文字列が対応付けられているか否かを判断する手段と、前記文字列が前記復帰先アドレスに対応付けられている場合、前記データが不正処理を実行するデータである旨の情報を出力する手段とを備えることを特徴とするデータ処理装置。

5. 複数の命令コードを含むデータの入力を受付ける手段を備え、該手段にて受付けたデータに含まれる命令コードに基づいて実行される処理が不正処理であるか否かを判断するデータ処理装置において、

所定の処理を実行する命令コード群を呼出するための命令コードを前記データから検索する手段と、前記命令コードが検索された場合、前記命令コード群の復帰先アドレスを取得するための命令コードが前記命令コード群に含まれるか否かを判断する手段と、前記命令コードが前記命令コード群に含まれる場合、前記データが不正処理を実行するデータである旨の情報を出力する手段とを備えることを特

徴とするデータ処理装置。

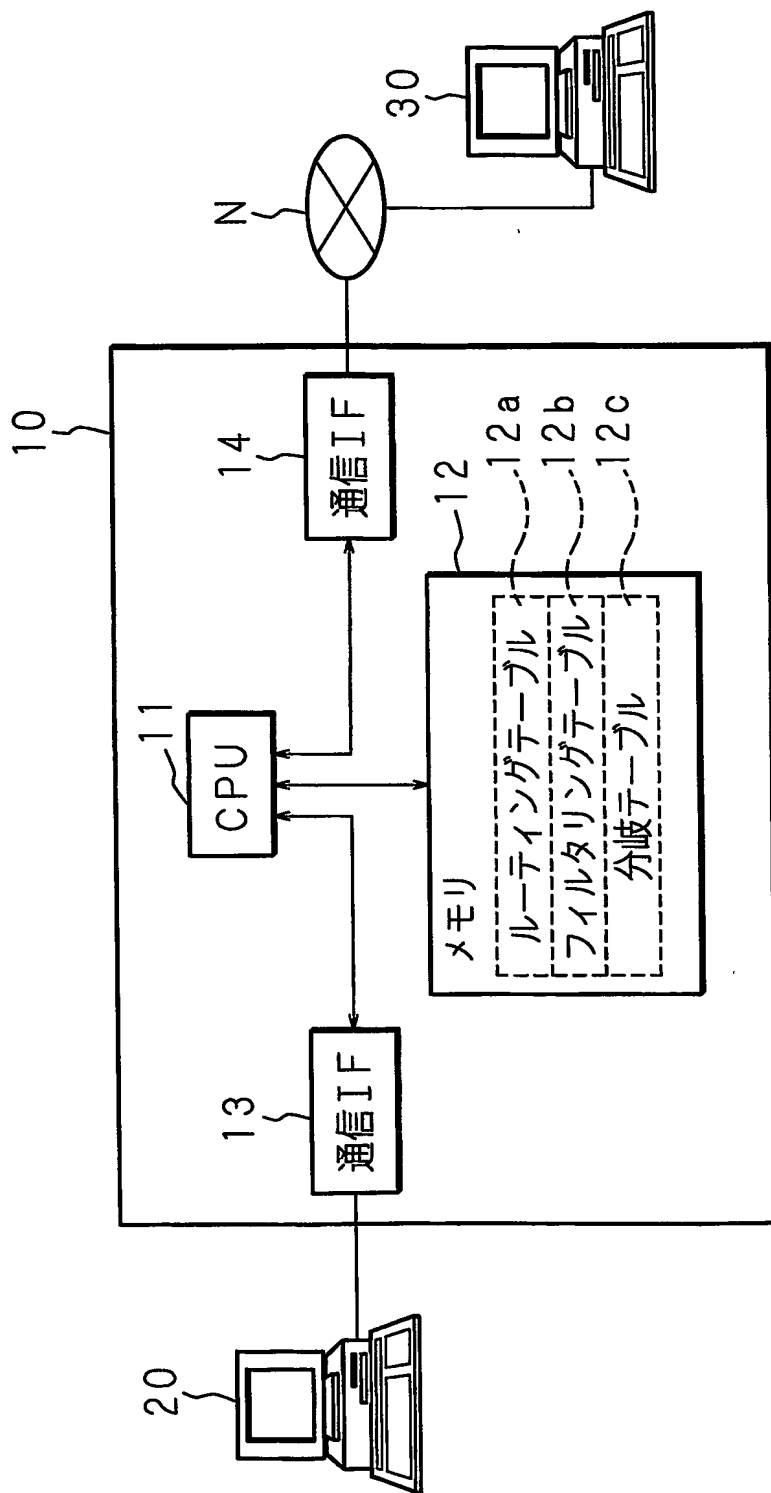
6. コンピュータに、入力された複数の命令コードを含むデータに基づいて実行される処理が不正処理であるか否かを判断させるステップを有するコンピュータプログラムにおいて、

コンピュータに、分岐命令に係る命令コードを前記データから検索させるステップと、コンピュータに、検索された命令コードに対応付けられている分岐元アドレス、及び前記命令コードの分岐先に対応付けられている分岐先アドレスを記憶させるステップと、コンピュータに、前記分岐先アドレスに、所定の処理を実行する命令コード群を呼出するための命令コードが対応付けられているか否かを判断させるステップと、コンピュータに、前記分岐先アドレスに前記命令コードが対応付けられていると判断した場合、前記命令コードの呼出先アドレスを記憶させるステップと、コンピュータに、記憶させた呼出先アドレスが前記分岐元アドレス及び分岐先アドレスの間にあるか否かを判断させるステップと有することを特徴とするコンピュータプログラム。

7. コンピュータに、入力された複数の命令コードを含むデータに基づいて実行される処理が不正処理であるか否かを判断させるステップを有するコンピュータプログラムが記録されているコンピュータでの読取りが可能な記録媒体において、

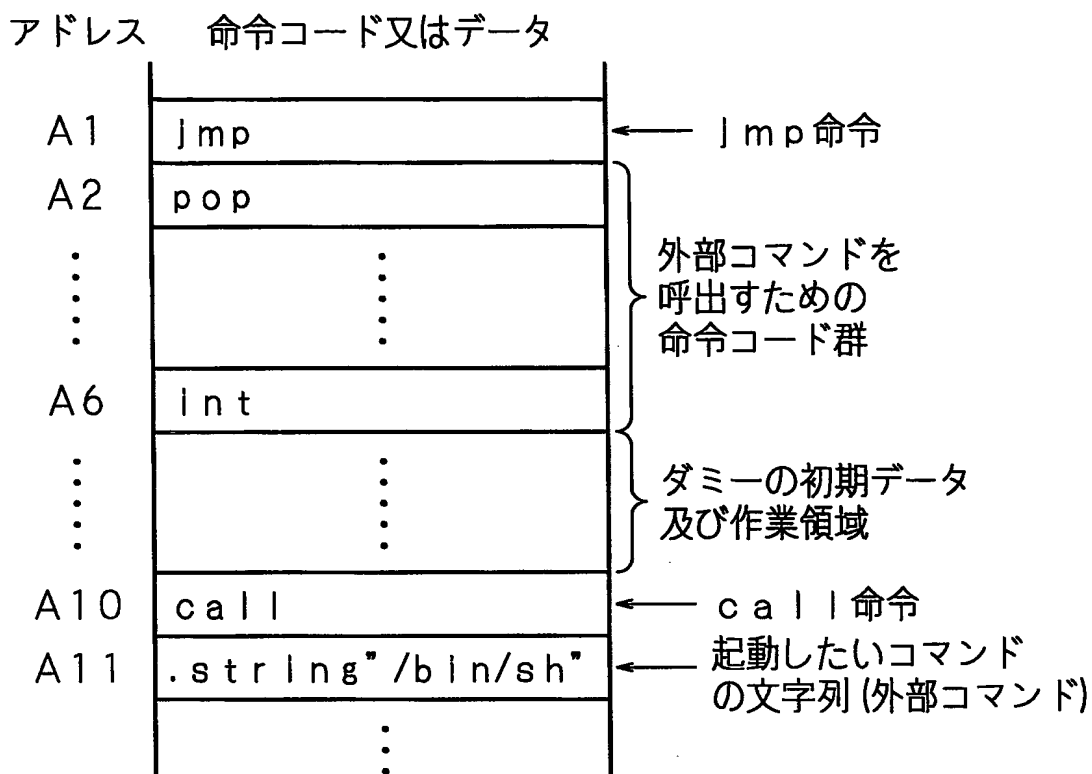
コンピュータに、分岐命令に係る命令コードを前記データから検索させるステップと、コンピュータに、検索された命令コードに対応付けられている分岐元アドレス、及び前記命令コードの分岐先に対応付けられている分岐先アドレスを記憶させるステップと、コンピュータに、前記分岐先アドレスに、所定の処理を実行する命令コード群を呼出するための命令コードが対応付けられているか否かを判断させるステップと、コンピュータに、前記分岐先アドレスに前記

命令コードが対応付けられていると判断した場合、前記命令コードの呼出先アドレスを記憶させるステップと、コンピュータに、記憶させた呼出先アドレスが前記分岐元アドレス及び分岐先アドレスの間にあるか否かを判断させるステップと有するコンピュータプログラムが記録されていることを特徴とするコンピュータでの読取りが可能な記録媒体。



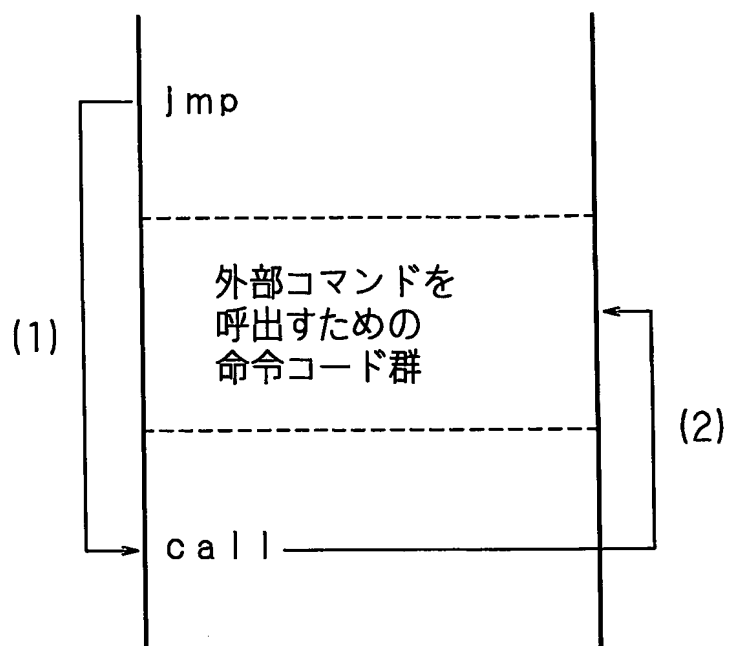
第 1 図

2 / 9



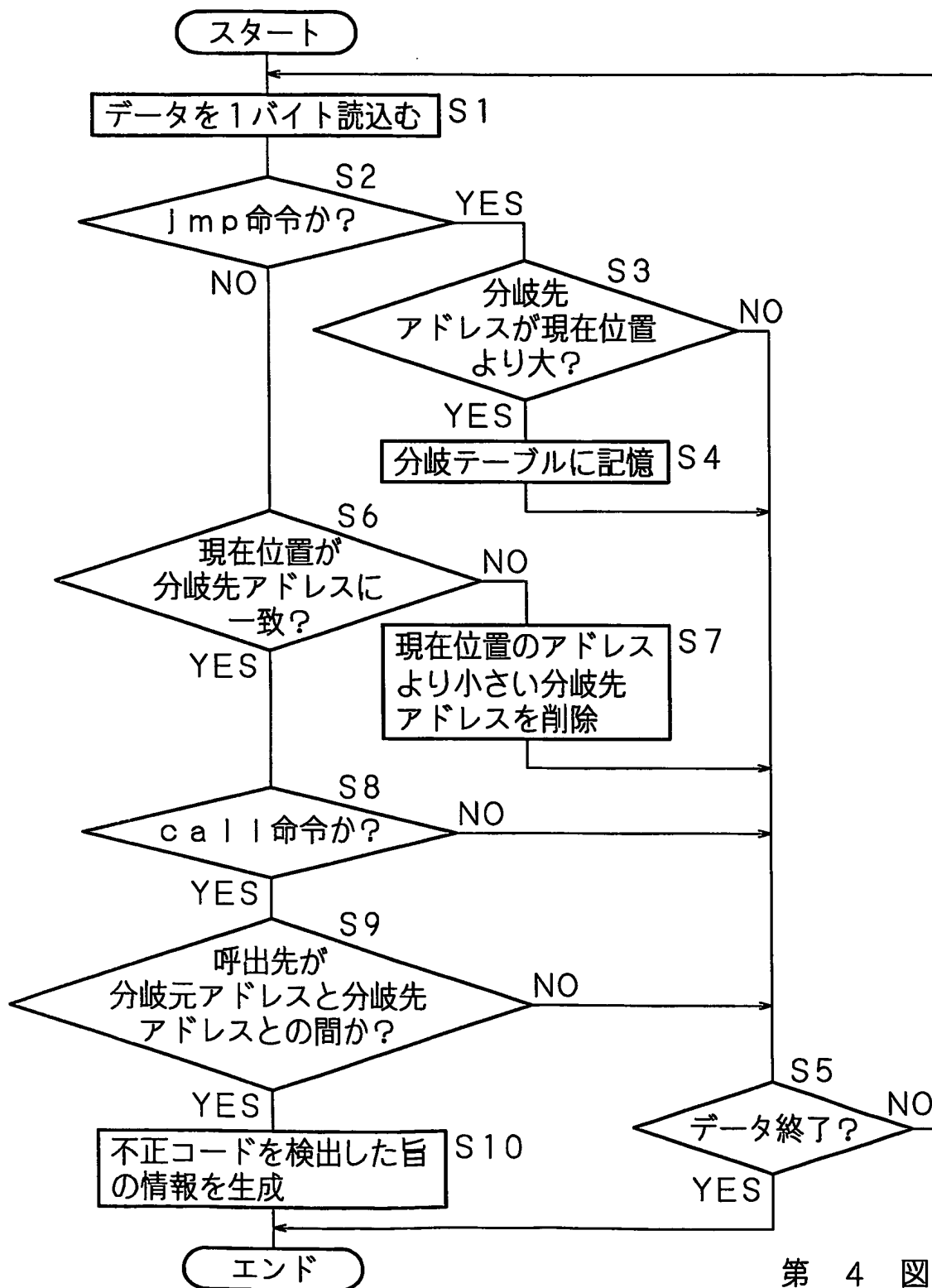
第 2 図

3 / 9



第 3 図

4 / 9

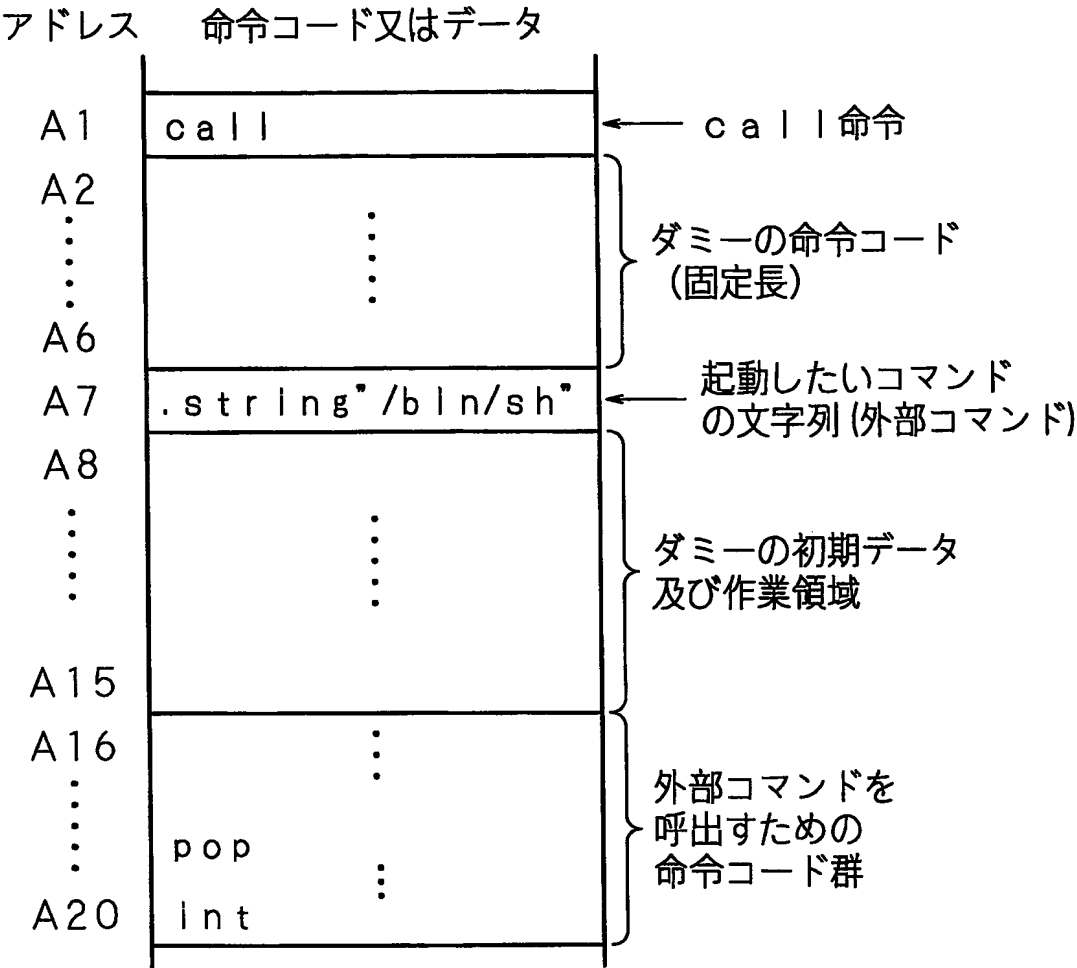


第 4 図

12c

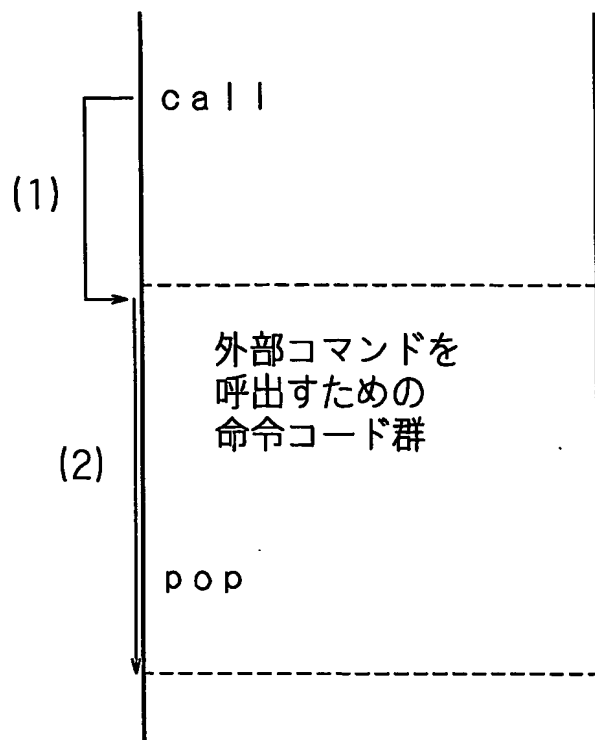
分岐元アドレス	分岐先アドレス
A 1	A 1 0
⋮	⋮

第 5 図



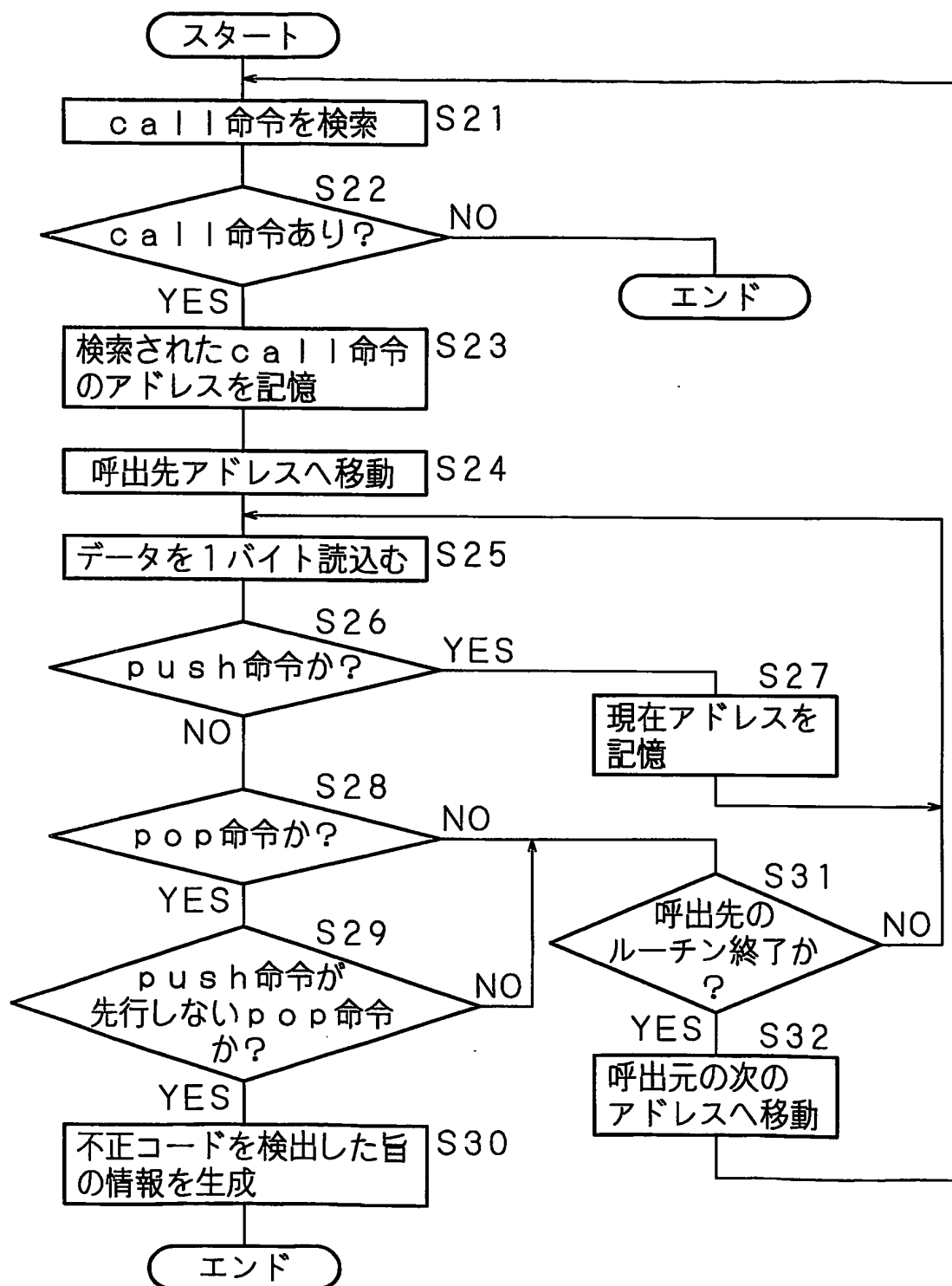
第 6 図

7/9

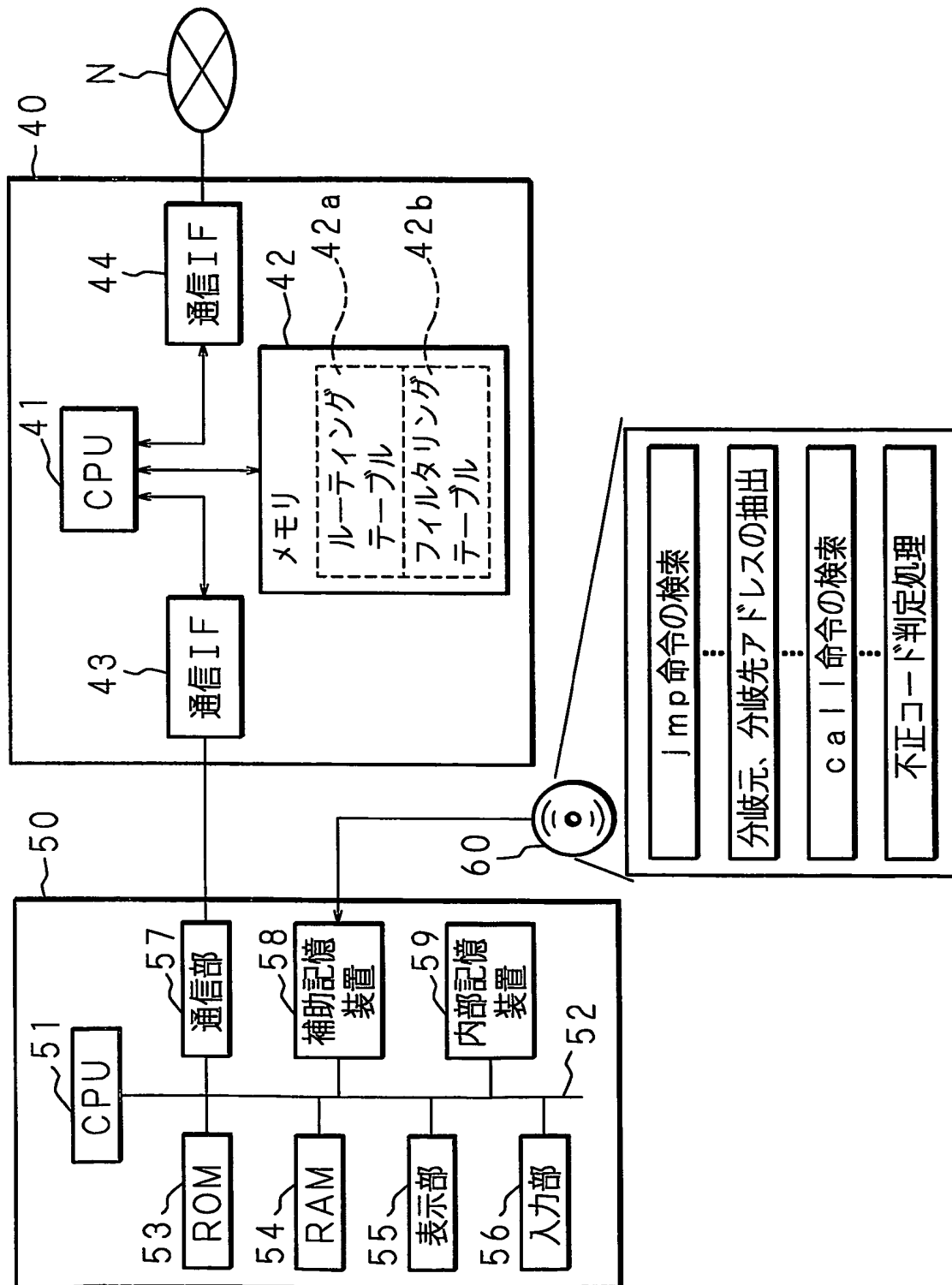


第 7 図

8/9



第 8 図



第 9 図

INTERNATIONAL SEARCH REPORT

International Application No.
PCT/JP03/09894

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ G06F11/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ G06F11/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2003
Kokai Jitsuyo Shinan Koho	1971-2003	Jitsuyo Shinan Toroku Koho	1996-2003

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Edited by Suguru YAMAGUCHI, 'Joho Security', first edition, Kyoritsu Shuppan Co., Ltd., (JP), 20 September, 2000 (20.09.00), pages 150 to 161	1-7
A	Written by Gakuto MASUDA, 'Computer Virus', first edition, Kabushiki Kaisha SCC, (JP), 16 January, 2000 (16.01.00), pages 108 to 110	1-7
A	Written by Palevich, J., translated by MAKINO, "E-Mail from Mountain View Dai 31 Kai Computer Virus no Subete", ASCII DOS/V ISSUE, (JP), 01 September, 1999 (01.09.99), Vol.5, No.9, pages 124 to 125	1-7

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to
"A" document defining the general state of the art which is not considered to be of particular relevance	understand the principle or theory underlying the invention
"E" earlier document but published on or after the international filing date	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"O" document referring to an oral disclosure, use, exhibition or other means	"&" document member of the same patent family
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search
02 October, 2003 (02.10.03)

Date of mailing of the international search report
14 October, 2003 (14.10.03)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl⁷ G06F11/00

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl⁷ G06F11/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996年
 日本国公開実用新案公報 1971-2003年
 日本国登録実用新案公報 1994-2003年
 日本国実用新案登録公報 1996-2003年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	山口英編、「情報セキュリティ」、初版、共立出版株式会社 (日)、2000.09.20、p.150-161	1-7
A	益田岳人著、「コンピュータ・ウィルス」、初版、株式会社SCC (日)、2000.01.16、p.108-110	1-7
A	Palevich, J. 著、牧野訳、"E-Mail from Mountain View 第31回 コンピュータウィルスのすべて" 、ASCII DOS/V ISSUE (日)、1999.09.01、第5巻、第9号、p.124-125	1-7

☐ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの
 「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
 「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
 「O」口頭による開示、使用、展示等に言及する文献
 「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日

02.10.03

国際調査報告の発送日

14.10.03

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)
 郵便番号100-8915
 東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

林 毅

印

5B

9193

電話番号 03-3581-1101 内線 3546